3F－03　バイオメトリクスを用いたユーザを識別しない認証方式の実装

飯田 恭弘　佐藤 直之　鈴木 英明
NTT 情報流通プラットフォーム研究所

1．はじめに

現在、Web 環境においては、ユーザ識別子とパスワードを用いてユーザの認証を行うことが多い。この手法では、Web ブラウザを利用しているユーザを識別し、識別されたユーザに対してあらかじめ登録された権利情報を用いて認証を実施している。しかし、本来認証の目的はユーザを識別することではなく、ユーザがある権利を持っているかどうかを確認することである。また逆に、ユーザを識別してしまうことは、プライバシ保護の点から好ましいとは言い難い。

本稿では、Web 上で個人を識別せずに個人の持つ権利のみを検証する手法を提案し、実現したので報告する。この手法には著者らがこれまでに提案してきた認証方式を用いている[1,2]。また、ユーザ端末の一部として指紋認証装置を使用した。

2．　認証方式の概要

まず、著者らがこれまでに提案してきた認証方式の概要を述べる。この認証方式では、ユーザを識別せずにその権利のみを証明する特殊な証明書を利用する。この証明書は発行を受けたユーザのみ利用可能であり、ユーザは証明書を何度でも利用することができる。また証明書を発行した発行局でさえ、証明書からはその証明対象となるユーザを識別できないという特徴がある。

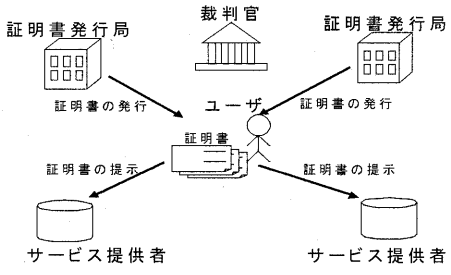

図１　モデル

本認証方式では図１に示す 4 種類の存在からなるモデルを提案している[1,2]。

(1) **証明書発行局** ： 証明書をユーザに発行する機関
(2) **サービス提供者** ： 証明書を検証しユーザへサービスを提供する機関
(3) **ユーザ** ： 認証の対象となる存在
(4) **裁判官** ： ユーザを識別し証明書を無効にできる唯一の機関

3．ソフトウェア構成

ユーザ用アプリケーションには証明書発行用および証明書検証用の二つがある。また、ユーザは Web ブラウザをインタフェースとして利用する。証明書発行サーバは WWW サーバと証明書を発行する発行サーバから構成される。サービス提供サーバは WWW サーバと証明書を検証する検証サーバから構成される。裁判官用アプリケーションには無効 ID リスト及び無効証明書リストを更新するためのアプリケーションがある。これらの無効リストは発行サーバおよび検証サーバへ配布される。

また、ユーザ端末にはソニー製の携帯可能な指紋認証装置 FIU-700（以下 FIU と呼ぶ）を接続している。同装置は指紋を用いてユーザの認証を行い、これに成功したユーザのみ、FIU 内に保存したデータの読み書きや、登録した秘密鍵を用いた計算が可能になるという機能がある。本実装においては、ユーザの証明書と、この認証方式において必要となるユーザの秘密鍵との両方を FIU に格納して管理している。このため、ユーザは安全に秘密鍵及び証明書を持ち運ぶことができる。

4. 証明書の発行

図２に従って証明書の発行処理を説明する。

①ユーザはユーザ端末の Web ブラウザを使用して証明書発行サーバの WWW サーバへアクセスする。

②WWW サーバは証明書を発行するための設定ファイルを Web ブラウザに返し、Web ブラウザはこのファイルの拡張子によりあらかじめ関連付けられた証明書発行用アプリケーションを起動する。

"An implementation of the anonymous authentication system using biometrics"
Yasuhiro IIDA, Naoyuki SATO, Hideaki SUZUKI
NTT Information Sharing Platform Laboratories

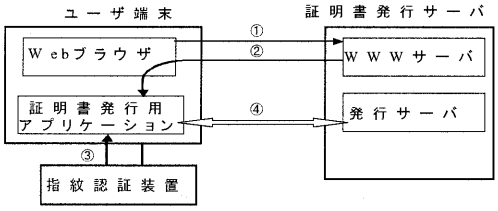

図2 証明書の発行

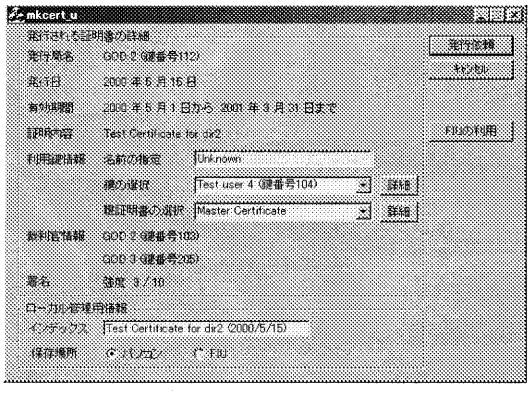

図3 証明書発行用アプリケーションの出力画面

③ユーザは指紋を用いて、FIU に対し本人性を証明する。これによってユーザは FIU に格納された秘密鍵および証明書を使用できるようになる。

④証明書発行用アプリケーションは証明書発行サーバとの間で証明書発行プロトコルを実施する。

図3は証明書発行用アプリケーションの出力画面のひとつである。

上記の一連の処理を実装して Web 上で権利のみを証明する証明書の発行が実現できることを確認した。

5. WWW サーバのディレクトリへのアクセス

図4に従って WWW サーバのディレクトリへのアクセス方法を説明する。

①ユーザはユーザ端末の Web ブラウザを使用して WWW サーバへアクセスする。

②WWW サーバは証明書を発行するための設定ファイルを Web ブラウザに返し、Web ブラウザはこのファイルの拡張子によりあらかじめ関連付けられた証明書検証用アプリケーションを起動する。

③ユーザは指紋を用いて、FIU に対し本人性を証明する。これによってユーザは FIU に格納された秘密鍵および証明書を使用できるようになる。

④証明書検証用アプリケーションは検証サーバとの間に証明書検証プロトコルを実施する。

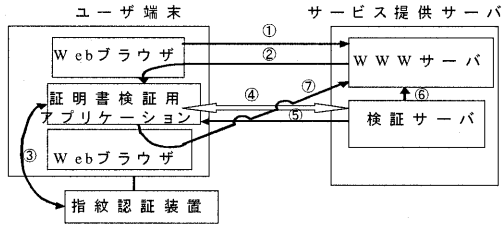

図4 WWW サーバのディレクトリへのアクセス

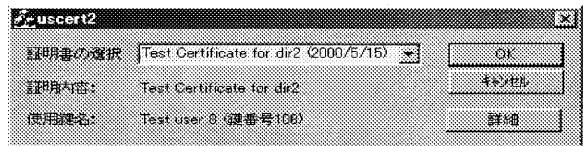

図5 証明書検証用アプリケーションの出力画面

⑤検証処理に成功すると、検証サーバは証明書検証用アプリケーションへ Web の Basic Authentication に使用するための一時的な ID とパスワードを発行する。

⑥また、検証サーバは⑤と同時に WWW サーバへこの ID とパスワードを登録する。

⑦証明書検証用アプリケーションは指定された ID とパスワードを引数の一部として新たに Web ブラウザを起動する。ユーザはこの Web ブラウザを用いて WWW サーバのディレクトリへアクセスする。

図5は証明書検証用アプリケーションの出力画面のひとつである。

上記の一連の処理を実装することにより、WWW サーバのディレクトリへのアクセスを個人を識別することなく権利のみに基づいて実現できることを確認した。

6. まとめ

今回、著者らは個人を識別せずにその権利のみを検証する認証方式を基盤として、権利の検証に成功したときのみ WWW サーバのディレクトリへアクセスできる手法を具体的に示した。また、本手法について指紋認証装置を使った実装を行い、有効性を確認した。今後は本実装の評価を行い、より効率的な実装についても検討する予定である。

参考文献

[1]佐藤直之, 鈴木英明, “匿名のままの権利行使を可能とした認証方式”, 情報処理学会論文誌, Vol.41, No.8, (2000)

[2]佐藤直之, 鈴木英明, “耐タンパ個人端末を利用し個人情報の保護を可能とした認証方式”, 情報処理学会論文誌, Vol.41, No.8, (2000)